Ideal Secret Sharing Schemes from Permutations

Josef Pieprzyk and Xian-Mo Zhang
(Corresponding author: Josef Pieprzyk)
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia. (Email: {josef, xianmo}@ics.mq.edu.au)

(Received Aug. 31, 2005; revised and accepted Oct. 11, 2005)

Abstract

The work presents a new method for the design of ideal secret sharing. The method uses regular mappings that are well suited for construction of perfect secret sharing. The restriction of regular mappings to permutations gives a convenient tool for investigation of the relation between permutations and ideal secret sharing generated by them.
Keywords: Ideal secret sharing schemes, perfect secret sharing schemes, permutations,

1 Introduction

Secret sharing allows a group of participants to collectively hold a secret. The secret is typically divided into shares and each participant has at least one share of the secret. Secret sharing is useful to protect secrets against a loss of the shares caused by unreliable storage but also can be used to enable a group to own secrets. The group ownership of a secret is of a great interest to cryptography as it can be used to handle cryptographic operations by groups rather than individuals.

There are many constructions of secret sharing schemes. The most prominent ones include the Shamir scheme [11] and Blakley schemes [2, 11]. These two constructions allow any group of n participants to share secret in such a way that any t ($t \leq n$) or more participants are able to recover jointly the secret (they are also called (t, n) threshold schemes). Ito, Saito, and Nishizeki gave a construction of perfect secret sharing for arbitrary monotone access structure [9]. An alternative construction of perfect secret sharing was given by Benaloh and Leichter [1].

Perfect secret sharing requires that any collection of participants not belonging to the access structure gains no information about the secret while any collection of participants from the access structure is able to recover the secret. Perfect secret sharing with shares of the same length as the secret is called ideal. Ideal secret sharing are of special practical interest as the storage of shares is the smallest possible. The best known construction of ideal secret sharing by Brickell [3] generalises the Shamir approach.

Secret sharing is originally defined on a finite field however it can be considered in a finite Abelian group so as to define black-box secret sharing [6, 7, 8].

In this work we give a new construction of ideal secret sharing. The construction is based on regular mappings. A mapping F from $GF(q)^t$ to $GF(q)^m$ is regular if F takes each vector $GF(q)^m$ precisely q^{t-m} times. Clearly, a regular mapping exists only when $t \geq m$. We are going to show that regular mappings provide perfectness when used to secret sharing construction. Moreover, as permutations are regular mappings for $t = m$, they generate ideal secret sharing. The work describes a new framework for the design of ideal secret sharing that can be seen as a generalisation of Brickell's approach [3].

The paper is structured as follows. The basic concepts of secret sharing are introduced in Section 2. Regular mappings and their properties are studied in Section 3. Section 4 explores properties of regular mappings in the context of the perfect and ideal secret sharing. In Section 5, we show a method to identify the coordinate functions of a permutation so that we can construct ideal secret sharing schemes. In Section 6, we extend the construction so as to obtain more ideal secret sharing schemes from a known one. Conclusions close the work.

2 Access Structures and Secret Sharing

A secret sharing scheme is a method to share a secret among a set of participants $\mathbf{P} = \{P_1, \ldots, P_n\}$. Let $\mathbf{K}$ denote the set of *secrets* and $\mathbf{S}$ denote the set of *shares*. The secret sharing has two algorithms: distribution algorithm (dealer) and recovery algorithm (combiner). The dealer assigns shares $s_1, \ldots, s_n$ to the participants $P_1, \ldots, P_n$, respectively. At the recovery stage, we assume that a collection of ℓ participants $P_{j_1}, \ldots, P_{j_\ell}$ is currently active and they send their shares $s_{j_1}, \ldots, s_{j_\ell}$ to the combiner. The combiner takes the submitted shares $s_{j_1}, \ldots, s_{j_\ell}$ and computes a secret. The secret is recovered if and only if $\{P_{j_1}, \ldots, P_{j_\ell}\}$ is a qualified subset of $\mathbf{P}$.

All qualified subsets of $\mathbf{P}$ create the *access structure* Γ.

An access structure Γ is said to be *monotone*

$$\text{if } \mathcal{A} \in \Gamma \text{ and } \mathcal{A} \subseteq \mathcal{B} \subseteq \mathbf{P} \text{ then } \mathcal{B} \in \Gamma.$$

We can describe the secret sharing scheme with the access structure Γ by an $m \times (n+1)$ matrix M^*, as introduced in [4, 5]. The matrix M^* has $n+1$ columns indexed by $0, 1. \ldots, n$. The value of m or the number of rows in M^* depends on the particular access structure Γ. We index the rows of the matrix M^* by $1, \ldots, m$. For a fixed i-th row of M^*, the entry on the 0-th position is the secret, and the i-th entry in the row shows the share s_i that is assigned to the participant P_i $(i = 1, \ldots, n)$. Let us denote the entry of the i-th row and the j-th column of M^* by $M^*(i, j)$. The matrix M^* is called a *defining matrix* of the secret sharing scheme with access scheme Γ. The matrix M obtained from M^* by removing the 0-th column is called the *associated matrix* of the scheme.

The dealer constructs the secret sharing by designing the defining matrix and choosing at random a row of the matrix M^*. Let it be the i_0-th row. The shares $M^*(i_0, j)$ are distributed to the corresponding participants P_j, $j = 1, \ldots, n$, and the secret is $M^*(i_0, 0)$.

A access structure $\Gamma = \{\mathcal{A} \mid \#\mathcal{A} \geq t\}$ is called a (t, n)-*threshold access structure*, where $\#\mathcal{A}$ denotes the number of elements in the set $\mathcal{A}$ and t is an integer with $0 < t \leq n$. A secret sharing scheme with a (t, n)- threshold access structure is called a (t, n)-threshold scheme. The parameter t is called the *threshold*.

Secret sharing is identified by its defining matrix. Clearly, permuting the rows of a defining matrix of a secret sharing scheme does not give a new scheme as the resulting matrix contains the same collection of rows. Permuting the columns of an associated matrix of secret sharing is equivalent to changing the indices of participants.

Given a secret sharing with the access structure Γ. We say that the secret scheme is *perfect* if the following two conditions are satisfied:

1) If $\mathcal{A} \in \Gamma$ then the participants in $\mathcal{A}$ recover the secret.

2) If $\mathcal{A} \notin \Gamma$ then the participants from $\mathcal{A}$ cannot recover any information about the secret (in an information theoretic sense).

As mentioned in [4], we can use the matrix M^* to express Conditions (1) and (2) more precisely as follows.

(a) Let $\mathcal{A} \in \Gamma$. If $M^*(i, j) = M^*(i', j)$ for every $P_j \in \mathcal{A}$ then $M^*(i, 0) = M^*(i', 0)$. The secret must be uniquely determined by the shares of qualified subset $\mathcal{A} \in \Gamma$.

(b) Let $\mathcal{A} \notin \Gamma$. For any integer $1 \leq i_0 \leq m$ and any $K \in \mathbf{K}$ there exists some integer i with $1 \leq i \leq m$ such that $M^*(i, j) = M^*(i_0, j)$ for all $P_j \in \mathcal{A}$ and $M^*(i, 0) = K$. The collection of shares of $\mathcal{A}$ matches many rows whose secrets run through all possible values of $\mathbf{K}$.

(b') Let $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\} \notin \Gamma$. For any $s_{j_1}, \ldots, s_{j_\ell} \in \mathbf{S}$ and any $K \in \mathbf{K}$, $\#\{i \mid M^*(i, j_u) = s_{j_u} \text{ for all } P_{j_u} \in \mathcal{A} \text{ and } M^*(i, 0) = K\}$ is independent of the choice of K. The unauthorised subset $\mathcal{A}$ knows nothing about the secret.

It is easy to verify that (b') implies (b). The secret sharing scheme satisfying (a) and (b) is called *weakly perfect*, while it is called *perfect* if it satisfies (a) and (b') [4]. It is known [5] that $\#\mathbf{K} \leq \#\mathbf{S}$ for perfect secret sharing. In particular, if $\#\mathbf{K} = \#\mathbf{S}$, the perfect secret sharing scheme is called *ideal*.

Let Γ be an access structure. $\mathcal{A} \in \Gamma$ is called *minimal* if any proper subset of $\mathcal{A}$ is not included in Γ. Clearly, Γ is uniquely determined by its minimal elements. Thus, to define an access structure Γ, it is sufficient to define all minimal elements of Γ. In particular, for a (t, n)-threshold scheme, clearly a subset of participants is minimal element if and only if it contains precisely t participants.

3 Regular Mappings

Let $q = p^v$ where p is a prime number and v is a positive integer. We write $GF(q)$ or $GF(p^v)$ to denote the finite field of $q = p^v$ elements, and $GF(q)^t$ or $GF(p^v)^t$ to denote the vector space of t tuples of elements from $GF(q)$. Note that each vector $\alpha \in GF(q)^t$ can be expressed as $\alpha = (a_1, \ldots, a_t)$ where $a_1, \ldots, a_t \in GF(q)$. The integer $a_1 q^{t-1} + \cdots + a_{t-1} q + a_t$ is called the *integer representation* of vector $\alpha = (a_1, \ldots, a_t)$, where each a_j and the sum are real-valued. Thus we can index all the q^t vectors in $GF(q)^t$:

$$\alpha_0, \alpha_1, \ldots, \alpha_{q^t - 1}$$

where j is the integer representation of α_j.

A mapping F from $GF(q)^t$ to $GF(q)^m$ $(t \geq m)$ is said to be *regular* if F takes each vector in $GF(q)^m$ precisely q^{t-m} times. Clearly in this case $t \geq m$. In particular, a regular mapping from $GF(q)^t$ to $GF(q)^t$ is exactly a permutation on $GF(q)^t$.

A *function* f on $GF(q)^t$ is a mapping from $GF(q)^t$ to $GF(q)$. The function f can be expressed as $f(x)$ or $f(x_1, \ldots, x_t)$, where $x = (x_1, \ldots, x_t) \in GF(q)^t$. The *truth table* of f is the sequence $f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q^t-1})$. Regular functions are called *balanced*.

Note that there are precisely q^{q^t} functions on $GF(q)^t$. On the other hand, we consider *polynomials* that can be expressed as

$$g(x_1, \ldots, x_t) = \sum a_{i_1, \ldots, i_t} x_1^{i_1} \cdots x_t^{i_t} \tag{1}$$

where each $a_{i_1, \ldots, i_t} \in GF(q)$, each i_j satisfies $0 \leq i_j \leq q-1$ as $a^q = a$ for any element $\alpha \in GF(q)$, and x_j^0 is defend as $x_j^0 = 1$. It should be pointed out that x_j^{q-1} and x_j^0 are not identical. By definition, if $i_j = 0$ then the term $x_1^{i_1} \cdots x_t^{i_t}$ does not contain x_j. On the other hand, $x_j^{q-1} = 0$ when $x_j = 0$ although $x_j^{q-1} = 1$ when $x_j \neq 0$. Since x_j^{q-1}

and x_j^0 are not identical, due to Equation (1), one can verify that there are precisely q^{q^t} polynomials on $GF(q)^t$. Therefore each function on $GF(q)^t$ can be expressed as a polynomial. This conclusion is useful in this work. If a function f can be expressed as $f(x_1, \ldots, x_t) = c + a_1x_1 + \cdots + a_tx_t$, then f is called an *affine function*. In particular, an affine function f is called *linear* if $c = 0$. It is easy to see that non-constant affine functions are balanced.

A mapping F from $GF(q)^t$ to $GF(q)^m$ $(t \geq m)$ can be expressed as

$$F(x_1, \ldots, x_t) = (f_1(x_1, \ldots, x_t), \ldots, f_m(x_1, \ldots, x_t)) \quad (2)$$

where each f_j is a function on $GF(q)^t$, called the j-th *coordinate function* of F.

The following statement is obvious.

Lemma 1 *The mapping (2) is regular if and only if for any integer k with $1 \leq k \leq m$ and any k coordinate functions $f_{i_1}, \ldots, f_{i_k}$, the mapping from $GF(q)^t$ to $GF(q)^k$,*

$$G(x_1, \ldots, x_t) = (f_{i_1}(x_1, \ldots, x_t), \ldots, f_{i_k}(x_1, \ldots, x_t))$$

is regular.

A characterisation of regular mappings can be found in Corollary 7.39 of [10]:

Lemma 2 *The mapping (2) is regular if and only if any nonzero linear combination of $f_1, \ldots, f_m$ is balanced, in other words, for any nonzero vector $(c_1, \ldots, c_m) \in GF(q)^t$, $c_1f_1 + \cdots + c_mf_m$ is balanced.*

Lemma 3 *The mapping (2) is regular if and only if for any $m \times m$ nonsingular matrix B over $GF(q)$, the mapping*

$$\begin{aligned} G(x_1, \ldots, x_t) &= (F(x_1, \ldots, x_t))B \\ &= (f_1(x_1, \ldots, x_t), \ldots, f_m(x_1, \ldots, x_t))B \end{aligned}$$

is a regular mapping from $GF(q)^t$ to $GF(q)^m$.

Combining Lemmas 1 and 3, we have

Lemma 4 *Let the mapping (2) be regular and $g_1, \ldots, g_k$ be linear combinations of $f_1, \ldots, f_m$. If g_1, …, g_k are linearly independent then*

$$H(x_1, \ldots, x_t) = (g_1(x_1, \ldots, x_t), \ldots, g_k(x_1, \ldots, x_t))$$

is a regular mapping from $GF(q)^t$ to $GF(q)^k$.

4 Ideal Secret Sharing from Regular Mappings

Let F be a regular mapping from $GF(q)^t$ to $GF(q)^m$ $(t \geq m)$. Then F can be expressed as

$$F(x_1, \ldots, x_t) = (f_1(x_1, \ldots, x_t), \ldots, f_m(x_1, \ldots, x_t)),$$

where f_j is the j-th coordinate function of F.

There precisely exist $q^m - 1$ nonzero linear combinations of $f_1, \ldots, f_m$, denoted by $g_1, \ldots, g_{q^m-1}$. We set

$$\Re_F = \{g_1, \ldots, g_{q^m-1}\}. \quad (3)$$

Clearly, $\Re_F$ forms a m-dimensional space and then the rank of $\Re_F$ is equal to m.

We now construct an ideal secret sharing scheme for n participants, $P_1, \ldots, P_n$.

Dealer (distribution algorithm)

- The dealer chooses $h_0, h_1, \ldots, h_n \in \Re_F$, not necessarily distinct, and defines an access structure Γ such that $\{P_{j_1}, \ldots, P_{j_\ell}\} \in \Gamma$ if and only if there is a sequence $c_1, \ldots, c_\ell \in GF(q)$ such that
$$h_0 = c_1h_{j_1} + \cdots + c_\ell h_{j_\ell}. \quad (4)$$
- The defining matrix M^* is created from h_i; $i = 0, \ldots, n$. The matrix has $(n+1)$ columns and q^t rows whose entries are from $GF(q)$, where $n+1 \leq q^m - 1$. The j-th column η_j of M^* is the truth table of h_j, $j = 0, 1, \ldots, n$.
- The dealer chooses at random a row of M^*. Let the index of the row be i, $1 \leq i \leq q^t$. The secret is $M^*(i, 0)$ and the shares are $M^*(i, 1), \ldots, M^*(i, n)$ that are distributed via secure channel to the corresponding participants. So P_j holds $s_j = M^*(i, j)$; $j = 1, \ldots, n$.

Combiner (recovery algorithm)

- The combiner takes the defining matrix M^* and collects shares sent from a group of currently active participants $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\}$.
- All rows containing the submitted shares are marked. When $\mathcal{A} \in \Gamma$, the corresponding secret will be identified and returned to each participant in $\mathcal{A}$. If $\mathcal{A} \notin \Gamma$, the marked rows contain secrets that are running through all values of $\mathbf{K}$ and the combiner is not able to determine the secret.

Lemma 5 *The defining matrix M^* of the secret sharing with the access structure Γ, defined in (4), satisfies Condition (a).*

Proof. Let $\{P_{j_1}, \ldots, P_{j_\ell}\} \in \Gamma$. Assume that $M^*(i, j_1) = M^*(i', j_1)$, …, $M^*(i, j_\ell) = M^*(i', j_\ell)$. Then $h_0 = c_1h_{j_1} + \cdots + c_\ell h_{j_\ell}$ for some $c_1, \ldots, c_\ell \in GF(q)$, and then $\eta_0 = c_1\eta_{j_1} + \cdots + c_\ell\eta_{j_\ell}$. It follows that $M^*(i, 0) = c_1M^*(i, j_1) + \cdots + c_\ell M^*(i, j_\ell)$ and $M^*(i', 0) = c_1M^*(i', j_1) + \cdots + c_\ell M^*(i', j_\ell)$. We have proved that $M^*(i, 0) = M^*(i', 0)$, and thus M^* satisfies Condition (a). □

Lemma 6 *The defining matrix M^* of the secret sharing with the access structure Γ, defined in (4), satisfies Condition (b').*

Proof. Let $\{P_{j_1}, \ldots, P_{j_\ell}\} \notin \Gamma$. Let M_1^* be the $q^t \times (\ell + 1)$ submatrix of M^*, comprised of $\ell + 1$ columns of M^*, indexed by 0, j_1, ..., j_ℓ. Similarly, let M_1 be the $q^t \times \ell$ submatrix of M^*, comprised of ℓ columns of M^*, indexed by j_1, ..., j_ℓ.

For any $K, s_1, \ldots, s_\ell \in GF(q)$, there are the two following cases: $(s_1, \ldots, s_\ell)$ is a row vector of M_1 and $(s_1, \ldots, s_\ell)$ is not a row vector of M_1.

Case 1: $(s_1, \ldots, s_\ell)$ is a row vector of M_1. Then there exists some $\alpha \in GF(q)^t$ such that

$$h_{j_1}(\alpha) = s_1, \ldots, h_{j_\ell}(\alpha) = s_\ell. \quad (5)$$

Let r denote the rank of $\{h_{j_1}, \ldots, h_{j_\ell}\}$. For conveniences, without loss of generality, we assume that $\{h_{j_1}, \ldots, h_{j_r}\}$ is a basis of $\{h_{j_1}, \ldots, h_{j_\ell}\}$, i.e., $h_{j_1}, \ldots, h_{j_r}$ are linearly independent and each of $h_{j_1}, \ldots, h_{j_\ell}$ can be uniquely expressed as a linear combination of $h_{j_1}, \ldots, h_{j_r}$. Set

$$H(x_1, \ldots, x_t) = (h_{j_1}(x_1, \ldots, x_t), \ldots, h_{j_r}(x_1, \ldots, x_t)).$$

Due to Lemma 4, H is a regular mapping from $GF(q)^t$ to $GF(q)^r$. Due to Lemma 1, we know that

$$h_{j_1}(\alpha) = s_1, \ldots, h_{j_r}(\alpha) = s_r$$

has precisely q^{t-r} solutions. Since each of $h_{j_{r+1}}, \ldots, h_\ell$ can be uniquely expressed as a linear combination of $h_{j_1}, \ldots, h_{j_r}$, we know that (5) has precisely q^{t-r} solutions.

On the other hand, recall that $\{P_{j_1}, \ldots, P_{j_\ell}\} \notin \Gamma$. Thus h_0 is not a linear combination of $h_{j_1}, \ldots, h_{j_r}$, and thus $h_0, h_{j_1}, \ldots, h_{j_r}$ are linearly independent. Set

$$H^*(x_1, \ldots, x_t) = (h_0(x_1, \ldots, x_t), h_{j_1}(x_1, \ldots, x_t), \ldots, h_{j_r}(x_1, \ldots, x_t))$$

Due to Lemma 4, H^* is a regular mapping from $GF(q)^t$ to $GF(q)^{r+1}$. Due to Lemma 1, we know that

$$h_0(\alpha) = K, h_{j_1}(\alpha) = s_1, \ldots, h_{j_r}(\alpha) = s_r$$

has precisely q^{t-r-1} solutions. Since each of $h_{j_{r+1}}, \ldots, h_\ell$ can be uniquely expressed as a linear combination of $h_{j_1}, \ldots, h_{j_r}$, we know that

$$h_0(\alpha) = K, h_{j_1}(\alpha) = s_1, \ldots, h_{j_\ell}(\alpha) = s_\ell$$

has precisely q^{t-r-1} solutions. Note that q^{t-r-1} is independent of the choice of K.

Case 2: $(s_1, \ldots, s_\ell)$ is not a row vector of M_1. In this case for any $K \in GF(q)$, clearly $(K, s_1, \ldots, s_\ell)$ does not appear in M_1^* as its a row vector no matter how to choose $K \in GF(q)$. So we have proved that Condition (b') is satisfied. □

According to Lemmas 5 and 6, we have the following theorem.

Theorem 1 *Let F be a regular mapping from $GF(q)^t$ to $GF(q)^m$ ($t \geq m$). For any integer n with $n+1 \leq q^m - 1$, the number of participants, and any $n+1$ nonzero linear combinations $h_0, h_1, \ldots, h_n$ of the coordinate functions $f_1, \ldots, f_m$ of F:*

1) *The secret sharing scheme with the access structure Γ, defined in (4), is perfect.*
2) *The matrix M^* is a defining matrix of the perfect secret sharing.*

Furthermore, we state

Corollary 1 *Let F be a regular mapping from $GF(q)^t$ to $GF(q)^m$ ($t \geq m$). For any integer n with $n+1 \leq q^m - 1$, the number of participants, and any $n+1$ nonzero linear combinations $h_0, h_1, \ldots, h_n$ of the coordinate functions $f_1, \ldots, f_m$ of F, the secret sharing scheme with the access structure Γ, defined in (4), is ideal, and $\mathbf{K} = \mathbf{S} = GF(q)$.*

Proof. Due to Lemma 2, each column of M^* must contain all elements in $GF(q)$. This proves that $\mathbf{K} = \mathbf{S} = GF(q)$. □

From (4), we need to determine all the coordinate functions of a given regular mapping so that we can construct a secret sharing scheme.

5 Finding Coordinate Functions of Permutations

When $t = m$, the regular mapping F from $GF(q)^t$ to $GF(q)^m$ is a permutation on $GF(q)^t$. As we have argued in Section 4, a permutation on $GF(q)^t$ can be used to construct ideal secret sharing schemes. We are going to focus our attention on permutations rather than on general regular mappings as permutations are easy to construct.

From a permutation χ on $GF(q^t)$, we can define a mapping F from $GF(q)^t$ to $GF(q)^t$ as follows. Let ϵ be a primitive element of degree t over $GF(q)$. For any $(c_1, \ldots, c_t) \in GF(q)^t$, let $\gamma = c_1\epsilon^{t-1} + \cdots + c_{t-1}\epsilon + c_t$, and let $\chi(\gamma) = d_1\epsilon^{t-1} + \cdots + d_{t-1}\epsilon + d_t$. We define $F(c_1, \ldots, c_t) = (d_1, \ldots, d_t)$. Clearly the mapping F is a permutation on $GF(q)^t$. We call F the *permutation reduced* by χ.

Example 1 *Let $q = 2$, $t = 3$. Define a function on $GF(2^3)$ such that $\chi(\gamma) = \gamma^3$ for any $\gamma \in GF(2^3)$. It is easy to verify that χ is a permutation on $GF(2^3)$. From χ, we now define a permutation F on $GF(2)^3$ as follows. Let ϵ be a root of the primitive polynomial $x^3 + x^2 + 1$. It is easy to verify that*

$$\begin{array}{ll} \chi(0) = 0, & \chi(1) = 1, \\ \chi(\epsilon) = \epsilon^2 + 1, & \chi(\epsilon + 1) = \epsilon, \\ \chi(\epsilon^2) = \epsilon^2 + \epsilon, & \chi(\epsilon^2 + 1) = \epsilon^2, \\ \chi(\epsilon^2 + \epsilon) = \epsilon^2 + \epsilon + 1, & \chi(\epsilon^2 + \epsilon + 1) = \epsilon + 1. \end{array}$$

We then define a permutation F on $GF(q)^3$ such that

$$\begin{array}{ll} F(0,0,0) = (0,0,0), & F(0,0,1) = (0,0,1), \\ F(0,1,0) = (1,0,1), & F(0,1,1) = (0,1,0), \\ F(1,0,0) = (1,1,0), & F(1,0,1) = (1,0,0), \\ F(1,1,0) = (1,1,1), & F(1,1,1) = (0,1,1). \end{array}$$

Set

$$F(x_1, x_2, x_3) = (f_1(x_1, x_2, x_3), f_2(x_1, x_2, x_3), f_3(x_1, x_2, x_3))$$

where f_j is a function on $GF(2)^3$. Then we can determine that

$$\begin{aligned} f_1(x_1, x_2, x_3) &= x_1 + x_2 + x_1x_2 + x_2x_3, \\ f_2(x_1, x_2, x_3) &= x_1 + x_1x_3 + x_2x_3, \\ f_3(x_1, x_2, x_3) &= x_2 + x_3 + x_1x_3. \end{aligned}$$

Assume that the secret sharing scheme contains four participants, P_1, P_2, P_3, P_4. We choose

$$h_0 = f_1,\ h_1 = f_2,\ h_2 = f_1 + f_3,$$
$$h_3 = f_2 + f_3,\ h_4 = f_1 + f_2 + f_3.$$

It is easy to verify that

$$\mathcal{B}_1 = \{h_3, h_4\},\ \mathcal{B}_2 = \{h_1, h_2, h_3\}$$

satisfy the following property that h_0 is a linear combination of the functions in each $\mathcal{B}_j$ but h_0 is not any linear combination of functions in any proper subset of $\mathcal{B}_j$. According to (4), we obtain an access structure Γ defined by its minimal elements

$$\mathcal{A}_1 = \{P_3, P_4\},\ \mathcal{A}_2 = \{P_1, P_2, P_3\}.$$

For each $\alpha \in GF(2)^3$, $h_0(\alpha)$ is the secret, $h_1(\alpha)$, $h_2(\alpha)$, $h_3(\alpha)$, and $h_4(\alpha)$ are the shares for P_1, P_2, P_3 and P_4 respectively. Due to Corollary 1, this secret sharing scheme with the access structure Γ, is ideal.

Example 2 *We consider a simple case of χ. Let χ be the identity permutation on $GF(3^4)$. Thus $F(x_1, x_2, x_3, x_4)$ is the identity permutation on $GF(3)^4$. We define a secret sharing scheme with seven participants, P_1, P_2, P_3, P_4, P_5, P_6, P_7, satisfying $\mathbf{K} = \mathbf{S} = GF(3)$. We choose*

$$\begin{aligned} &h_0(x) = x_1 + x_2 + x_3 + x_4, && h_1(x) = x_1, \\ &h_2(x) = x_2, && h_3(x) = x_3, \\ &h_4(x) = x_4, && h_5(x) = x_1 + x_2, \\ &h_6(x) = x_1 + x_4, && h_7(x) = x_2 + x_4 \end{aligned}$$

It is easy to verify that

$$\begin{aligned} &\mathcal{B}_1 = \{h_1, h_2, h_3, h_4\}, && \mathcal{B}_2 = \{h_1, h_3, h_5, h_6\}, \\ &\mathcal{B}_3 = \{h_2, h_3, h_5, h_7\}, && \mathcal{B}_4 = \{h_3, h_4, h_6, h_7\}, \\ &\mathcal{B}_5 = \{h_3, h_4, h_5\}, && \mathcal{B}_6 = \{h_2, h_3, h_6\}, \\ &\mathcal{B}_7 = \{h_1, h_3, h_7\} \end{aligned}$$

satisfy the following property that h_0 is a linear combination of the functions in each $\mathcal{B}_j$ but h_0 is not any linear combination of functions in any proper subset of $\mathcal{B}_j$. Due to (4), we obtain an access structure Γ defined by its minimal elements:

$$\begin{aligned} &\mathcal{A}_1 = \{P_1, P_2, P_3, P_4\}, && \mathcal{A}_2 = \{P_1, P_3, P_5, P_6\}, \\ &\mathcal{A}_3 = \{P_2, P_3, P_5, P_7\}, && \mathcal{A}_4 = \{P_3, P_4, P_6, P_7\}, \\ &\mathcal{A}_5 = \{P_3, P_4, P_5\}, && \mathcal{A}_6 = \{P_2, P_3, P_6\}, \\ &\mathcal{A}_7 = \{P_1, P_3, P_7\} \end{aligned}$$

For any $\alpha \in GF(3)^4$, $h_0(\alpha)$ is a secret, and each $h_j(\alpha)$ is the share for participant P_j, $j = 1, \ldots, 7$. For example, let $\alpha = (2, 1, 0, 2)$. Then the secret is $K = 2$, the shares for $P_1, P_2, P_3, P_4, P_5, P_6, P_7$ are 2, 1, 0, 2, 0, 1, 0 respectively. Due to Corollary 1, we obtain an ideal secret sharing scheme with the access structure Γ.

6 Extended Constructions

In this section, we construct other secret sharing schemes from the one, constructed in Section 4.

Theorem 2 *Let M^* be a defining matrix of the secret sharing scheme with the access structure Γ defined in (4). For any integer j' with $1 \le j' \le n$ and any integer k with $1 \le k \le v - 1$, where $q = p^v$, we replace each entry c in the j'-th column by c^{p^k}, where p is the characteristic of $GF(q)$, i.e., $q = p^v$. Denote the resulting matrix by M^{**}. Then M^{**} is a defining matrix of an ideal secret sharing scheme with the same access structure Γ.*

Proof. Let $P_1, \ldots, P_n$ be all the participants and $P_{j_1}, \ldots, P_{j_\ell}$ be all the currently active participants. Let M_1^* be a $q^t \times \ell$ submatrix of M^*, comprised of ℓ columns of M^*, indexed by $j_1, \ldots, j_\ell$, where $1 \le j_1 < \cdots < j_\ell \le n$. We now verify that M^{**} satisfies Conditions (a) and (b').

There two cases to be considered: $j' \notin \{j_1, \ldots, j_\ell\}$ and $j' \in \{j_1, \ldots, j_\ell\}$. For the first case: $j' \notin \{j_1, \ldots, j_\ell\}$, clearly both (a) and (b') are satisfied. We next consider the second case: $j' \in \{j_1, \ldots, j_\ell\}$. Without loss of generality, we assume that $j' = j_\ell$.

We first verify Condition (a). Let $\{j_1, \ldots, j_\ell\} \in \Gamma$. Assume that

$$\begin{aligned} M^{**}(i, j_1) &= M^{**}(i', j_1), \ldots, M^{**}(i, j_{\ell-1}) \\ &= M^{**}(i', j_{\ell-1}), \\ M^{**}(i, j_\ell) &= M^{**}(i', j_\ell) \end{aligned}$$

Then

$$\begin{aligned} M^{*}(i, j_1) &= M^{*}(i', j_1), \ldots, M^{*}(i, j_{\ell-1}) \\ &= M^{*}(i', j_{\ell-1}), \\ M^{**}(i, j_\ell) &= M^{**}(i', j_\ell). \end{aligned}$$

Note that $M^{**}(i, j_\ell) = (M^*(i, j_\ell))^{p^k}$ and $M^{**}(i', j_\ell) = (M^*(i', j_\ell))^{p^k}$. Note that

$$c^{p^k} = b^{p^k} \text{ if and only if } c = b. \tag{6}$$

Hence $M^*(i, j_\ell) = M^*(i', j_\ell)$. Summarising the above, we have

$$\begin{aligned} M^{*}(i, j_1) &= M^{*}(i', j_1), \ldots, M^{*}(i, j_{\ell-1}) \\ &= M^{*}(i', j_{\ell-1}) \\ M^{*}(i, j_\ell) &= M^{*}(i', j_\ell). \end{aligned}$$

Due to Corollary 1, M^* is a defining matrix of an ideal secret sharing scheme. Hence $M^*(i, 0) = M^*(i', 0)$ and

hence $M^{**}(i,0) = M^{**}(i',0)$. This proves that M^{**} satisfies Condition (a).

We next verify Condition (b'). Let $\{j_1, \ldots, j_\ell\} \notin \Gamma$. For any fixed $K, s_{j_1}, \ldots, s_{j_\ell} \in GF(q)$, we consider

$$\begin{aligned} M^{**}(i,j_1) &= s_{j_1}, \ldots, M^{**}(i,j_\ell) \\ &= s_{j_\ell} \\ M^{**}(i,0) &= K. \end{aligned} \quad (7)$$

Clearly (7) is equivalent to

$$\begin{aligned} M^{*}(i,j_1) &= s_{j_1}, \ldots, M^{*}(i,j_{\ell-1}) \\ &= s_{j_{\ell-1}}, \\ M^{**}(i,j_\ell) &= s_{j_\ell} \\ M^{*}(i,0) &= K. \end{aligned} \quad (8)$$

Due to (6) there uniquely exists $c \in GF(q)$ such that $c^{p^k} = s_{j_\ell}$. Thus (8) is equivalent to

$$\begin{aligned} M^{*}(i,j_1) &= s_{j_1}, \ldots, M^{*}(i,j_{\ell-1}) \\ &= s_{j_{\ell-1}}, M^{*}(i,j_\ell) \\ &= c \\ M^{*}(i,0) &= K. \end{aligned} \quad (9)$$

Since M^* is a defining matrix of a perfect secret sharing, the number of i satisfying (9) is independent of the choice of K. Equivalently, the number of i satisfying (7) is independent of the choice of K. We have verified Condition (b') for M^{**}. Thus we have proved that the secret sharing scheme with defining matrix M^{**} is perfect. Since $\mathbf{K} = \mathbf{S} = GF(q)$, this secret sharing scheme is ideal. From the above we can conclude that the access structure of the secret sharing scheme with the defining matrix M^{**} is also Γ. □

It should be noted that, in Theorem 2, the ideal secret sharing scheme with the defining matrix M^{**} and the ideal secret sharing scheme with the defining matrix M^* have the same access structure Γ. However Γ satisfies (4) with defining matrix M^*, while Γ may not satisfy (4) with the defining matrix M^{**}.

Applying the same reasoning as in the proof of Theorem 2 to the 0-th column of M^*, we have

Theorem 3 *Let M^* be a defining matrix of the secret sharing scheme with the access structure Γ defined in (4). Let k be an integer with $1 \le k \le v-1$. We replace each entry c in the 0-th column by c^{p^k}. Denote the resulting matrix by M^{**}. Then M^{**} is a defining matrix of an ideal secret sharing scheme with the same access structure Γ.*

Using the same argument repeatedly, we have

Theorem 4 *Let M^* be a defining matrix of the secret sharing scheme with the access structure Γ defined in (4). For any integer r with $1 \le r \le n+1$, any integers $1 \le k_1, \ldots, k_r \le v-1$, where $q = p^v$, and any integers $0 \le j_1 < \cdots < j_r \le n$, we replace each entry c in the j_u-th column by $c^{p^{k_u}}$, $u = 1, \ldots, r$. Denote the resulting matrix by M^{**}. Then M^{**} is a defining matrix of an ideal secret sharing scheme with the same access structure Γ.*

7 Limitations of Constructions

Let F be a regular mapping from $GF(q)^t$ to $GF(q)^m$. Due to Theorem 1, for a given n, the number of participants, and $n+1$ linear combinations $h_0, h_1, \ldots, h_n$ of the coordinate functions $f_1, \ldots, f_m$ of F, we can construct an ideal secret sharing scheme with an access structure Γ, where Γ is identified by $h_0, h_1, \ldots, h_n$ and (4). We show that the construction is subject to some limitations.

Lemma 7 *Let F be a regular from $GF(q)^t$ to $GF(q)^m$ ($t \ge m$), n be an integer with $n+1 \le q^m - 1$, $h_0, h_1, \ldots, h_n$ be $n+1$ nonzero linear combinations of the coordinate functions $f_1, \ldots, f_m$ of F, and Γ be an access structure, defined in (4). If $\mathcal{A} = \{P_{j_1}, \ldots, P_{j_\ell}\}$ is a minimal element in Γ, then $\ell \le m$.*

Proof. We first prove that $h_{j_1}, \ldots, h_{j_\ell}$ are linearly independent. Assume that $h_{j_1}, \ldots, h_{j_\ell}$ are linearly dependent. Then h_0 can be linearly expressed by a basis $\{h_{i_1}, \ldots, h_{i_r}\}$ of $\{h_{j_1}, \ldots, h_{j_\ell}\}$, where $r < \ell$. Due to (4), $\{P_{i_1}, \ldots, P_{i_r}\} \in \Gamma$. Note that $\{P_{i_1}, \ldots, P_{i_r}\} \subset \mathcal{A}$. This contradicts the condition that $\mathcal{A}$ is a minimal element in Γ. The contradiction proves that $h_{j_1}, \ldots, h_{j_\ell}$ are linearly independent. Recall that the rank of $\Re_F$, where $\Re_F$ has been defined in (3), is equal to m. Hence $\ell \le m$. □

Lemma 7 shows that a restriction on the size of minimal elements in any access structure Γ, defined in (4).

8 Conclusions

We have shown how regular mappings from $GF(q)^t$ to $GF(q)^m$ can be applied to construct perfect and ideal secret sharing schemes. We have given a method to find all the coordinate functions of a permutation so that we can construct ideal secret sharing schemes from this permutation. Furthermore, from a single implementation of ideal secret sharing scheme, we can construct other ideal secret sharing schemes with the same access structure.

Acknowledgement

The authors were supported by Australian Research Council grants DP0345366 and DP0451484.

References

[1] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *CRYPTO'88*, LNCS 403, pp. 27-36, Springer-Verlag, 1988.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceeding AFIPS 1979 National Computer Conference*, pp. 313-317, AFIPS, 1979.

[3] E. F. Brickell, "Some ideal secret sharing schemes," *Journal of Computer and Systems Science*, vol. 37, pp. 156-189, 1988.

[4] E. F. Brickell and D. M. Davenport, "On the classification of ideal secret sharing schemes," *Journal of Cryptology*, vol. 4, pp. 123-134, 1991.

[5] E. F. Brickell and D. R. Stinson, "Some improved bounds on information rate of perfect sharing schemes," *Journal of Cryptology*, vol. 5, pp. 153-166, 1992.

[6] R. Cramer and S. Fehr, "Optimal block-box secret sharing over Abelian groups," in *CRYPTO'02*, LNCS 2442, pp. 272-287, Springer-Verlag, 2002.

[7] Y. Desmedt and Y. Frankel, "Hreshold cryptosystem," in *CRYPTO'89*, LNCS 435, pp. 307-315, Springer-Verlag, 1990.

[8] Y. Desmedt and Y. Frankel, "Homomorphic zero-knowledge threshold schemes over any finite Abelian group," *SIAM Journal on Discrete Mathematics*, vol. 7, no. 4, pp. 667-679, 1994.

[9] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *IEEE Globecom '87*, pp. 99-102, IEEE, 1987.

[10] R. Lidl and H. Niederreiter, *Finite fields, encyclopedia of mathematics and its applications*, Cambridge, U. K.: Cambridge University Press, 1983.

[11] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612-613, Nov. 1979.

Josef Pieprzyk received BSc in Electrical Engineering from Academy of Technology in Bydgoszcz, Poland, MSc in Mathematics from University of Torun, Poland, and PhD degree from Polish Academy of Sciences in Warsaw. Josef Pieprzyk is a Professor in the Department of Computing, Macquarie University, Sydney, Australia.

Josef Pieprzyk published 5 books, edited 10 books (conference proceedings published by Springer-Verlag), 3 book chapters, and 160 papers in refereed journals and refereed international conferences. He is a member of the editorial board for International Journal of Information Security (published by Springer-Verlag). Professor Pieprzyk is a sought after reviewer for many international journals (including Journal of Cryptology; IEEE Transactions on Information Theory; IEEE Computer; IEE Proceedings; Computers and Digital Techniques; Designs, Codes and Cryptography; Discrete Applied Mathematics; Discrete Mathematics, etc.). He was serving as Program Chair for 7 international conferences, was a member of Program Committees for more than 30 international conferences. He also supervised 13 PhD students who completed successfully their studies.

His research interest includes computer network security, database security, design and analysis of cryptographic algorithms, algebraic analysis of block and stream ciphers, theory of cryptographic protocols, secret sharing schemes, threshold cryptography, copyright protection, e-Commerce and Web security. Josef Pieprzyk is a member of IACR.

Xian-Mo Zhang received the M.Sc degree in mathematics from Nankai University, Tianjin, China, in 1982, and the Ph.D degree in mathematics and computer science from University College, the University of New South Wales, Canberra, Australia, 1992.

During 1992-2001, he was with the University of Wollongong, Wollongong, Australia, first as a research assistant then as a Queen Elizabeth II Fellow. He is currently a research fellow at Macquarie University, Sydney, Australia. His research interests include combinatorics and cryptography.